Overview

• HIPAA Audits
• HHS/OCR Settlement Agreements
• OCR’s Focus for 2017

HIPAA Audit Preparedness

Elizabeth G. Litten, Esq.

May 12, 2017
HCCA New York Regional Conference
New York, NY
HIPAA Audits

www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/phase2announcement/index.html

2016 Phase 2 HIPAA Audit Program Continues

Goal: audit 200-250 Covered Entities (CEs) and Business Associates (BAs)

- Emails verifying contact information received in spring of 2016
- Subset received “Audit Pre-Screening Questionnaire” in spring/summer of 2016 (20 questions)
- 167 CEs selected via randomized selection algorithm for desk audits (BA selection was to have occurred in fall 2016)
- Subset of CEs selected for 2017 on-site audits

Phase 2 HIPAA Audit Program, cont.

- Desk Audit HIPAA Controls: 7 Areas of Focus
  - NPP content and practices – 45 CFR 164.520(a)(i) and (b)(1)
  - NPP electronic notice requirements – 164.520(c)(3)
  - Patients' right to access PHI – 164.524
  - Timeliness of breach notification – 164.404(b)
  - Content of breach notification – 164.404(c)(1)
  - Security Risk Analysis – 164.308(a)(3)(i)(A)
Phase 2 HIPAA Audit Program, cont.

- OCR Q/A Insights:
  - Desk audit may be Privacy-focused or Security-focused
  - Required submission of Privacy Policies and Procedures
  - Required submission of Security Risk Assessments (current, previous year, 6 years ago)
  - Lack of cooperation with desk audit could trigger on-site audit
  - If CE has multiple locations and audit letter is received by administrative office, all locations are subject to the audit
  - Privacy audit will confirm NPP is consistent with access P&Ps

Who Is Being Audited?

- Covered Entities
- Business Associates
- Individuals and Organizations
- Large and Small
- Entities “All Sizes and Functions”

How Does OCR Pick?

- Want a broad spectrum of candidates. Entities of all sizes and functions.
- OCR has an algorithm with sampling criteria:
  - Size
  - Type
  - Operations
  - Affiliations/relationship with other health care organizations
  - Public/private
  - Geography
- Did not select entities that had current open complaint investigation or undergoing a compliance review by OCR.
The Process

- Contact Info Verification Letter (or email)
- Pre-Screening Questionnaire sent to gather additional data about size, type, and operations
- Identification of Business Associates (spreadsheet)
- OCR selected entities for HIPAA Audit through random sampling; selected auditees were notified by email of their participation

“Communications from OCR will be sent via email and may be incorrectly classified as spam. If your entity’s spam filtering and virus protection are automatically enabled, we expect you to check your junk or spam email folder for emails from OCR.”

Alert: Phishing Email Disguised as Official OCR Audit Communication - November 28, 2016

It has come to our attention that a phishing email is being circulated on behalf of OCR. Departmental letterhead may be altered to appear as if it came from OCR. The email appears to be an official governmental communication, and typically impersonates a HIPAA audit. The email is intended to trick recipients into clicking on a link that directs them to a fake HIPAA website. The email claims to contain a HIPAA Audit Notice, and contains a malicious link that will infect their computer.

OCR would like to further state that this phishing email originates from the email address DMS0102420@f.hhs.gov and includes a link to a site, which contains malware. If you are a subscriber to the official HIPAA email address or the email address of a HIPAA audit recipient, DMS00102420@f.hhs.gov, but have received this email, please delete it immediately and do not click on any links or open any attachments.

If your organization has any questions or to verify if you have received an official communication from our agency regarding HIPAA audit, please contact us at [email protected] or [email protected]

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/
What Is the Status of Audits?

- **DESK Audits**
  - Auditees submitted documentation via a "secure audit portal"
  - Round 1 = Covered Entities
  - Round 2 = Business Associates
  - Round 1 desk audits are complete
  - No information yet from OCR about generalized findings

- **ONSITE Audits** – Round 3.
  - Covered Entities and Business Associates
  - Onsite Audits slated to commence in 2017
  - Might request certain information be submitted via OCR portal
  - Will examine a broader scope of requirements

OCR’s Focus for 2017

- Continuation with HIPAA Audits – Onsite Visits
- Modernizing HIPAA and Supporting Innovation in Healthcare –
  - Efforts to "modernize" health information privacy and security protections through expanded guidance and regulatory change
  - Enable further advances in health care, research, and technology that will improve health outcomes and improve ability to detect and prevent cyber-attacks
  - OCR Guidance on HIPAA and Cloud Computing (October 2016) – identifying cloud services providers (CSPs) as business associates (to extent they receive or maintain PHI) and addressing situations in which CSPs experience security events

Select 2017 Compliance Areas:

1. Access Rights

- HHS FAQs (https://www.hhs.gov/hipaa/professionals/privacy/guidance/access/finalreleasedfaqs) and Audit item 3 of 7 emphasize focus on individual right to access PHI
- Access v. Authorization (don’t use latter when request is for Access!)
- Right to access (most) PHI in Designated Record Set
- May require request to be in writing, if CE informs individual of the requirement
- Reasonable verification – cannot create barriers or unreasonable delay
  - May not require individual to physically come to office if mailing requested
  - May not require use of web portal
Select 2017 Compliance Areas:
(1) Access Rights, cont.

- May provide summary, if individual agrees in advance
- Expected that all CEs can readily produce and provide via email
  - Must send via unencrypted email, if requested by individual
  - Must provide brief warning that there is “some level of risk” while in transit
- Form and format of request
  - Paper records must be provided electronically, if so requested, if "readily producible" (i.e., can scan)
Select 2017 Compliance Areas:
(3) Security Policies

- Enterprise-wide Risk Analysis and Security Policies
  - Media and Device Policies & Procedures (BYOD restrictions; secure network use)
  - Security Awareness and Training for Workforce
  - User attestations
  - Encryption!

- MAPFRE Life – 2017 $2.2M “Resolution Amount” and CAP
  - Unencrypted pen drive stolen from IT department overnight results in breach affecting 2,209 individuals

Select 2017 Compliance Areas:
(4) Health Apps

Mobile Health App: is App Developer Your BA?

- Patient downloads health app to smartphone and inputs health information – HIPAA does not apply, because app developer is not creating, receiving, maintaining or transmitting PHI as a CE or BA/Subcontractor
- Patient downloads health app to smartphone because provider makes app available to patients – HIPAA applies because developer is BA of provider

Select 2017 Compliance:
(5) Cloud Service Providers

- Encryption is not enough – CSP maintaining PHI is a Business Associate, as per HHS
- The “blindfolded Business Associate” – CSP may not know it holds PHI – must verify the type of data it holds, particularly if encrypted
- Service Level Agreement must be consistent with HIPAA and Business Associate Agreement (https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html?language=es)
Select 2017 Compliance Areas:
(6) Telehealth/Telemedicine

- Effective 1/1/17, CMS using new POS code 02 for telehealth and reimburse using facility rate for Method II Critical Access Hospital
- Consider Joint Commission requirements for secure texting as possible model for secure telehealth platform

Select 2017 Compliance Areas:
(7) BAs and Big Data

- Does BAA permit Data Aggregation?
- Is BA performing Data Aggregation on behalf of CE?
  - “Data Aggregation” means, with respect to BA, combining of CE’s PHI with PHI of another CE “to permit data analyses that relate to the health care operations of the respective” CEs (45 CFR 164.501)
  - “Health Care Operations” means activities of CE including quality assessment and improvement; review of competence of health care professionals; medical review, legal services, auditing; business management activities of CE (45 CFR 164.501)

HIPAA Settlements
## OCR Resolution Agreements

1. July 16, 2008: Providence Health & Services ($100k)
2. January 16, 2009: CVS Pharmacy, Inc. ($2.25M)
3. July 27, 2010: Rite Aid Corporation ($1M)
5. February 4, 2011: Cigna Maryland ($4.3M) [CMP]
6. February 14, 2011: Gem Hospital & Mass General Phys ($1.5M)
7. July 6, 2011: UCLA Health System ($865.500K)
8. March 13, 2012: BCBS Tennessee ($1.5M)
9. April 13, 2012: Phoenix Cardiac Surgeons ($100K)
10. June 26, 2012: Alaska DHSS ($1.7M)
11. September 17, 2012: Mass Eye & Ear Associates
12. December 31, 2012: Hospice of Northern Idaho ($50K)

## Case Examples & Resolution Agreements (continued)

13. May 21, 2013: Idaho State University ($400K)
14. June 13, 2013: St. Maria Regional Medical Center ($770K)
15. July 11, 2013: WellPoint ($1.7M)
16. August 14, 2013: Affinity Health Plan ($1,215,780)
17. Dec 26, 2013: Adult/Pediatric Dermatology P.C. ($150K)
19. April 22, 2014: QHC Health Plan Inc. ($250K)
20. April 22, 2014: Concentra Health Services ($1,725,220)
21. May 7, 2014: NY and Presbyterian Hospital ($3.3M)
22. May 7, 2014: Columbia University ($1.5M)
23. June 21, 2014: Parkview Health System ($865K)
25. April 22, 2015: Cornell Prescription Pharm ($125K)
26. June 10, 2015: St. Elizabeth Medical ($218,400)
27. August 31, 2015: Cancer Care Group ($750K)
28. November 24, 2015: Lebanon Hospital ($50K)
29. November 30, 2015: Triple-S Corp ($5.5M)
30. December 1-4, 2015: Univ of Washington ($750K)
31. February 3, 2016: Lincare, Inc ($239,800)
32. February 16, 2016: Pool & Land PT ($25K)
33. March 16, 2016: North Memorial Health Care
34. March 17, 2016: Polkinstem Institute ($3.8M)
35. April 14, 2016: Raleigh Ortho Clinic ($70K)
36. April 21, 2016: NY Presbyterian ($2.2M)
Case Examples & Resolution Agreements (continued)

37. June 29, 2016: Catholic Health Services (BA) ($650K)
38. July 14, 2016: Oregon Health & Science Univ ($2.7M)
39. July 21, 2016: Univ of Mississippi Medical ($2.75M)
40. August 4, 2016: Advocate Health ($5.55M)
41. September 23, 2016: Care New England Health ($400K)
42. October 17, 2016: St. Joseph Health ($2.14M)
43. November 22, 2016: Univ of Massachusetts Amherst ($600,000)
44. January 9, 2017: Presence Health ($475,000)
45. January 18, 2017: MAPFRE Life Insurance Company of Puerto Rico ($2.2M)
46. February 2, 2017: Children's Medical Center of Dallas ($3.2M)
47. February 16, 2017: Memorial Healthcare Systems ($5.5M)

Rise in Enforcement Activity

• Over 7 years of enforcement. As of Feb. 28, 2017:
  – OCR has received over 150,000 HIPAA complaints
  – OCR has investigated and resolved almost 25,000 cases, requiring corrective action
  – OCR has settled 47 cases, resulting in total penalties of over $67.2 Million
• 2016 was a record setting year:
  – HIPAA Enforcement actions: 13
    (prior record: 7 in 2014)
  – Collections on HIPAA enforcement: $23 Million
    (prior record: $7.4 Million in 2014)
  – Single largest fine for HIPAA violations: $5.5 Million
    (prior record: $4.8 Million in 2011 (Cignet Health: $4.3M -- $1.3M for violations & $3M for failing to cooperate with investigation))
OCR Enforcement

• Compliance issues investigated most are, in order of frequency:
  ‒ Impermissible uses and disclosures of protected health information;
  ‒ Lack of safeguards of protected health information;
  ‒ Lack of patient access to their protected health information;
  ‒ Use or disclosure of more than the minimum necessary protected health information; and
  ‒ Lack of administrative safeguards of electronic protected health information.

OCR Enforcement

• The most common types of covered entities that have been required to take corrective action are, in order of frequency:
  ‒ Private Practices;
  ‒ General Hospitals;
  ‒ Outpatient Facilities;
  ‒ Pharmacies; and
  ‒ Health Plans (group health plans and health insurance issuers).

Enforcement Lessons Learned From OCR

• Encrypt laptops and mobile devices, including thumb drives!
  ‒ Providence Health ($100K)
  ‒ Idaho Hospice ($50K)
  ‒ Mass Ear/Eye MDs ($1.5M)
  ‒ Alaska DHSS ($1.7M)
  ‒ Concentra ($1.725M) (if you don’t, document the alternative used)
  ‒ QCA ($250K)

• Dispose of PHI properly, including wiping leased copiers of ePHI!
  ‒ CVS ($2.25M)
  ‒ Rite Aid ($1M)
  ‒ Affinity Health ($1.2M) (purge ePHI from copiers & devices)
  ‒ Parkview Health System ($1M) (don’t leave PHI in driveways)

• Don’t take PHI off-site!
  ‒ Gen Hospital Corp. & Mass Gen MD Org ($1.5M)

• Enter into BA Agreements with vendors who store or secure your PHI!
  ‒ BCBS Tennessee ($1.5M)
  ‒ AZ Cardiologists ($1M)
Enforcement Lessons Learned

- Perform and Update Security Risk Assessments, especially with system upgrades
  - BCBS Tenn ($1.5M)
  - Idaho State Univ ($400K)
  - Wellpoint ($1.7M)
  - Columbia ($1.8) / NY Presbyterian ($3.3M)
  - Anchorage ($1.75K) (don't use outdated software, and fail to update patches)
- Ensure you have Control Policies over your Devices and Media (Cancer Care)
- Apply Minimum Necessary to disclosure within organization! (Shasta Medical)
- Train & Sanction Employees, including executives (Shasta Medical $275K)
- CORRECT Violations!
  - Cignet Maryland ($4.3M)
  - UCLA (Fiscal)
- Cooperate with OCR! Cignet Maryland ($4.3M)

HIPAA as the “Standard of Care”

- At least 10 States (Delaware, Connecticut, Kentucky, Maine, Minnesota, Montana, North Carolina, Tennessee, Utah, West Virginia) have published judicial decisions and precedent supporting that a court may at least look to HIPAA when considering the relevant standard of care for State privacy violation claims brought by individuals.
- Byrne v. Avery Center for Obstetrics and Gynecology, the Connecticut Supreme Court went one step further and concluded that HIPAA regulations can establish the standard of care in certain situations!
Bryne v. Avery Center for Obstetrics and Gynecology, P.C.

• Facts: Emily Byrne, asked Avery Center for Obstetrics and Gynecology not to provide her PHI to her significant other (HIPAA’s Request for Restriction). The Center received a subpoena from her significant other’s attorneys in a paternity suit, and promptly turned over the information without alerting the patient or fighting the subpoena in court.
  - Byrne sued Avery Center for negligence, but a lower court ruled that HIPAA preempted the negligence suit. Byrne then appealed.
  - Holding: November 2014, the Connecticut Supreme Court overruled the lower court and pointed to language in the preamble to the final HIPAA to permit privacy lawsuits based on State law to go forward. HIPAA does not preempt State law cases of action.
  - Impact: De facto right of action under HIPAA, which could subject health care providers to more lawsuits for breaching patient confidentiality.

Developments on the Horizon

• Premera (currently ongoing)
  - Insurer suffered data breach that went undetected for over a year, leading to dissemination of sensitive information for approx. 11 million individuals
  - Plaintiffs argue, in part, that NPP is a contract between insurer and consumers
  - In August, Court dismissed certain negligence and breach of contract claims; however, certain claims still unsettled:
    • Fraud allegations regarding statements in the company’s privacy notice, code of conduct and other materials provided to consumers; and
    • Breach of contract claims for the statements in the company’s privacy notice and “Preferred Select” policy (under Oregon law; claims based on Washington law dismissed)
  • Unjust enrichment claim, alleging that it was unjust for Premera to retain fees for health insurance without securing sensitive data.

HIPAA Take-Aways and Reminders

• Due diligence for sale of covered entity: beware of Data Room disclosures!
• Data aggregation in the “big data” era: does your BAA permit it?
• Patient access rights v. authorization and preemption of state laws regarding copy charges
• Medical device hacking
• Health apps: is it PHI?
Thank You. Any Questions?

Elizabeth G. Litten, Esq.
Fox Rothschild LLP
elitten@foxrothschild.com
https://hipaahealthlaw.foxrothschild.com
609.895.3320